Department of Homeland Security
Information Analysis and Infrastructure Protection
Daily Open Source Infrastructure Report
for 08 April 2004

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

For info click here
www.whitehouse.gov/homeland

Daily Overview

- vnunet.com reports the Anti−Phishing Working Group is warning of a new type of phishing attack: when users click on a link in an e−mail pretending to come from their bank or another company, they are sent to a fake Website which will then try to steal bank account details or other information. (See item 4)

- The Associated Press reports an Amtrak train jumped its tracks in a swampy area of the Mississippi Delta, killing a 68−year−old passenger and injuring more than 60 other people. (See item 5)

- vnunet.com reports that security vendor F−Secure is urging users to patch their systems after the discovery of two flaws in a version of its anti−virus software that leaves users vulnerable to hackers and virus writers. (See item 23)

DHS/IAIP Update *Fast Jump*

Production Industries: Energy; Chemical; Defense Industrial Base

Service Industries: Banking and Finance; Transportation; Postal and Shipping

Sustenance and Health: Agriculture; Food; Water; Public Health

Federal and State: Government; Emergency Services

IT and Cyber: Information and Telecommunications; Internet Alert Dashboard

Other: General; DHS/IAIP Web Information

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) – http://esisac.com]

1. *April 07, Associated Press* — **Kerr−McGee buying Westport Resources for $2.5 billion in stock. Energy explorer Kerr−McGee Corp. said Wednesday it is buying Denver−based Westport Resources Corp. for about $2.5 billion in stock in a deal that would create one of the biggest independent oil and gas producers in the United States.** The acquisition will

boost Kerr−McGee's holdings in oil and natural gas reserves in the Rockies and southern Texas, a move company officials said will make output more predictable and raise daily production volume by more than 34 percent. Westport stockholders will receive 0.71 shares of Oklahoma City−based Kerr−McGee stock for each share of Westport. That values Westport shares at $36.57 a share, or 11 percent above Tuesday's closing Westport price of $33.05. Kerr−McGee expects to issue 49.4 million new shares to Westport's shareholders. Those shares were valued at about $2.5 billion at Tuesday's close. The company will also assume about $900 million of Westport debt.

Source: http://biz.yahoo.com/ap/040407/na_fin_com_us_kerr_mcgee_west_port_2.html

2. *April 07, KRT Wire* — **LNG controversy in Baja California heats up. The controversy over plans to develop liquefied natural gas (LNG) receiving terminals in Baja, CA, has ratcheted up a notch, with Mexico's two major opposition parties challenging a project for the first time.** Leaders of the former ruling party, the Institutional Revolutionary Party, or PRI, and the Party of the Democratic Revolution, or PRD, are opposing ChevronTexaco's plan to put a floating LNG receiving terminal next to the Coronado Islands. They contend the project would violate Mexico's sovereignty and compromise its national security. If ChevronTexaco gets all its permits, construction would begin this year and be completed by 2007. The facility would receive liquefied natural gas shipments in tankers from Australia's Gorgon fields, re−gasify the fuel and send it through an undersea pipeline to the Baja, CA and California natural gas grids.

Source: http://www.miami.com/mld/miamiherald/business/national/83776 37.htm?1c

[Return to top]

Chemical Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

3. *April 07, Government Computer News* — **Defense pushes for a single RFID standard.** The Department of Defense (DoD) is coordinating its rollout of radio−frequency ID (RFID) tags with other federal organizations in hope of arriving at a single set of standards. Ed Coyle, chief of the Defense Logistics Agency's Automatic Identification Technology Office, spoke Wednesday, April 7, at the RFID Summit for Industry in Washington. He said DoD is coordinating its use of RFID with the Food and Drug Administration, General Services Administration, Postal Service, and Transportation Security Administration. **DoD has mandated that all of its suppliers must place passive RFID tags on pallets and cases shipped to the department after January 2005. DoD wants to play a strong role in directing development of RFID technology to ensure that its specifications will be compatible with those used by the private sector.** Coyle assured DoD suppliers at the conference that the data constructs being developed for the government's RF tags will be the same as those used by Wal−Mart and other large commercial enterprises, which are beginning to require RF tags on their shipments.

Source: http://gcn.com/vol1_no1/daily−updates/25517−1.html

Banking and Finance Sector

4. *April 08, vnunet.com (UK)* — **Online phishing uses new bait.** The Anti−Phishing Working Group (APWG) is warning of a new type of phishing attack. When a user clicks on a link in an e−mail pretending to come from their bank or another company, they are sent to a fake Website which will then try to steal bank account details or other information. The new trick uses software that detects the user's browser and applies custom JavaScript to replace the look and feel of the web address bar with an appropriately designed working fake, to fool people into thinking they are visiting a legitimate site. **The second issue with a fake address bar is the possibility for a 'man in the middle' attack, where every subsequent website visited, and any passwords or credit card numbers entered, could be sent to the phisher until the browser window is closed.** "We've seen about 30 unique attacks using this basic source code since 25 February 2004," said the APWG spokesman.
Source: http://www.vnunet.com/News/1154101

Transportation Sector

5. *April 07, Associated Press* — **Amtrak passenger dies during train derailment. An Amtrak train jumped its tracks in a swampy area of the Mississippi Delta, killing a 68−year−old passenger and injuring more than 60 other people. The nine−car train, traveling from New Orleans to Chicago, derailed Tuesday night, April 6, near the town of Flora, tumbling off a trestle five or six feet approximately 25 miles north of Jackson.** Many rescuers were forced to use off−road vehicles to reach the accident site because of woods and soggy ground. Searchers used flash lights and portable lighting as they moved from car to car checking for more injured. Dan Stessel, a spokesman for Amtrak, said 68 passengers and 12 crew members were on the train, the City of New Orleans. He said he had no information on what caused the accident. All passengers and crew were accounted for late Tuesday. Stokes said that while the derailment was believed to be an accident, the FBI had sent agents to the scene. Gov. Haley Barbour declared a state of emergency. The train consisted of one engine, one baggage car, seven passenger cars and one unoccupied passenger car. Amtrak said all nine cars derailed, with the first seven coming to rest on their sides. The locomotive remained on the track.
Source: http://www.ajc.com/news/content/news/ap/ap_story.html/Nation al/AP.V7969.AP−Amtrak−Derailme.html

6. *April 07, Associated Press* — **Three dozen federal workers at the Miami airport have been taken to the hospital.** Officials say a strange odor caused some of them to suffer eye irritation and nausea. **A concourse was closed for about two hours after the Transportation Security Administration workers complained about the fumes at a security checkpoint.** Hazardous materials workers haven't been able to detect any chemicals or strange fumes. The investigation

continues.Officials don't believe there was any sabotage. They say early reports indicate carbon monoxide may be responsible. No passengers were affected.
Source: http://www.wavy.com/Global/story.asp?S=1769263

7. *April 06, Federal Computer Week* — **TSA to test passenger fast lane.** Up to 10,000 volunteers will be scanned for biometric characteristics in a pilot test of a program to find more detailed ways to screen travelers. Transportation Security Administration (TSA) officials said today, April 6, that they want to test a program designed to bolster security and increase efficiency in screening travelers at airports nationwide. Rear Adm. David Stone, acting administrator of TSA, announced that the agency is seeking proposals from companies for a registered traveler pilot test that will begin at a few airports in late June. The contract will be awarded in early June. **The pilot will test biometric technology such as iris scanners and possibly fingerprint readers to see whether they enhance security and efficiency. TSA officials are looking for biometric systems that are ready to use, accurate, cost effective and capable of confirming the identities of large populations quickly.** The pilot program is expected to use 5,000 to 10,000 volunteer travelers. If everything works well, officials expect people taking part in the program will pass through airport security more quickly than other travelers.
Source: http://www.fcw.com/fcw/articles/2004/0405/web−tsa−04−06−04.a sp

[Return to top]

Postal and Shipping Sector

8. *April 05, DM News* — **Time becomes factor in postal reform passage.** Though mailers still expect postal reform bills to be introduced shortly, many are growing less confident that legislation will be passed before the end of the year because of the fall elections. **House Government Reform Committee chairman Tom Davis, R−VA, will introduce a postal reform bill by the end of the month with Rep. John McHugh, R−NY, who chairs the House committee's postal panel, a McHugh spokesperson said.** Senate Governmental Affairs Committee chairwoman Susan Collins, R−ME, plans to introduce legislation with Sen. Thomas Carper, D−DE, that would be out of committee by May. **After the bills are introduced, however, many steps remain before legislation would be signed into law.** "I don't think we can say with any certainty that a postal reform bill is going to pass or it's not going to pass this year," said Bob McLean, executive director of the Mailers Council. Congress has only through July to work on legislation before summer recess. Lawmakers also aren't in session numerous days in September, and the targeted adjournment for this session of Congress is October 1.
Source: http://www.dmnews.com/cgi−bin/artprevbot.cgi?article_id=2704 6

[Return to top]

Agriculture Sector

9. *April 07, Associated Press* — **Sudden oak death found in Georgia. The state Department of Agriculture says the fungal disease that causes sudden oak death has been found in plants sold by five nurseries in Georgia.** In March, Agriculture Commissioner Tommy Irvin

quarantined shipments from California, where the disease has killed tens of thousands of oaks. After the quarantine, samples were taken from plants shipped from California. **About 500 samples are being tested from more than 50 nurseries that received suspect plants, Irvin said.** He said the confirmed cases were in camellias grown by Monrovia Nursery, and "we expect there will be more positives." Florida and Oregon also have found positive samples, he said.
Source: http://www.accessnorthga.com/news/ap_newfullstory.asp?ID=356 76

10. *April 07, Associated Press* — **Citrus quarantine. Florida agriculture officials declared a new citrus canker quarantine for nearly 18 square miles of Boynton Beach after they found and removed infected trees on more than 124 properties in the city.** Workers from the state's canker eradication program have destroyed all of the infected trees as well as other citrus trees on those properties. They also have destroyed about 200 trees on neighboring properties that they considered exposed to canker. The canker bacteria causes brown blemishes on fruit and can cause the tree to drop fruit prematurely and eventually die. The quarantine bars residents, nursery owners, and landscapers from planting or moving citrus trees or keeping potted citrus plants within the affected area.
Source: http://www.news−press.com/news/local_state/040407citrus−upda te.html

[Return to top]

Food Sector

11. *April 07, Food and Drug Administration* — **Foodborne illness guide for health care workers released.** Americans' vulnerability to foodborne illness has been highlighted by large outbreaks over the last two years. To increase awareness, a new educational guide for health care professionals on how to identify and treat foodborne illnesses, as well as consumer tips for patients, was released April 7. "Approximately 76 million Americans suffer from a foodborne illness every year, and 5,000 deaths each year are attributed to foodborne illness," said Cecil B. Wilson, American Medical Association Trustee. "Health care professionals are the front−line of prevention. Arming physicians with the latest information on foodborne illnesses helps them better diagnose and treat their patients." **The guide,"Diagnosis and Management of Foodborne Illnesses: A Primer for Physicians and Other Health Care Professionals" contains charts, scenarios, and a continuing medical education section and is free to health care professionals. The primer, initially introduced in 2001, contains five new sections on new and re−emerging foodborne illnesses and was written with an emphasis on living in the post 9−11 environment.**
Source: http://www.fda.gov/bbs/topics/news/2004/NEW01047.html

[Return to top]

Water Sector

12. *April 07, Billings Gazette (Montana)* — **Study: Canada takes too much water. Canadian irrigators have been wrongfully taking 90,000 acre−feet of Montana water a year for more than 80 years, a state study shows, and Governor Judy Martz is pushing to**

renegotiate the international agreement that created the problem. The issue dates to 1921, when U.S. and Canadian officials signed an agreement to share the waters of the St. Mary and Milk rivers. Both rivers have their headwaters in Montana's Glacier National Park and flow north into Canada. The Milk River later flows back into Montana north of Havre. From there, it runs east and forms the economic lifeline of Hi–Line agriculture all the way to Glasgow, said Richard Moy, chief of the Water Management Bureau in Montana's Department of Natural Resources and Conservation. About 140,000 acres of Montana farmland are irrigated with Milk River water, Moy said, and the crops grown there make up about 8 percent of Montana's agriculture economy. **The 1921 order called for the two rivers to be considered one stream, with each country receiving half of its water. An analysis submitted by Montana officials last December to a joint U.S. and Canadian board that oversees the agreement shows that Montana routinely ends up on the short end of the stick.** That's because the Milk River routinely runs dry and the St. Mary rarely does.
Source: http://www.billingsgazette.com/index.php?id=1&display=rednews/2004/04/07/build/state/25–canada–water.inc

[Return to top]

Public Health Sector

13. *April 06, Canadian Press* — **WHO starts process of developing human vaccine to British Columbia avian flu strain.** The World Health Organization (WHO) is starting the process of producing a human vaccine for the H7 avian flu virus ravaging poultry stocks in British Columbia, Canada. **They will try to develop what's called a viral seed, a genetically modified version of the H7 virus that could be used by commercial vaccine makers should the H7 strain emerge as a pandemic strain.** That appears unlikely at this point, but nevertheless health authorities have to prepare for the possibility. It's also good practice for when the next pandemic, believed by influenza experts to be inevitable. **WHO pandemic planning guidelines require the organization to commence production on a human vaccine for an avian influenza strain once there is evidence two people have been infected in an outbreak,** a WHO spokesperson explained.
Source: http://story.news.yahoo.com/news?tmpl=story&cid=1843&ncid=1843&e=9&u=/cpress/20040406/ca_pr_on_he/avian_flu_vaccine

14. *April 06, University of Illinois at Urbana–Champaign* — **Gene with key role in replicating pox viruses also halts inflammation.** Scientists at the University of Illinois at Urbana–Champaign studying vaccinia virus, a close relative of smallpox, have determined that a gene necessary for virus replication also has a key role in turning off inflammation, a crucial anti–viral immune response of host cells. **The discovery potentially broadens the knowledge base of how all poxviruses cause disease and how they may be outwitted by improvements in vaccines against them,** said Joanna L. Shisler, a professor of microbiology at Urbana–Champaign. "If we can find out how the virus evades immune responses and learn more about the signals the virus sees as necessary for replicating within the host cell, then we can figure out how to inhibit them and halt the viral replication," she said.
Source: http://www.eurekalert.org/pub_releases/2004–04/uoia–gwk04060 4.php

[Return to top]

Government Sector

Nothing to report.
[[Return to top]]

Emergency Services Sector

15. *April 07, Government Technology* — **Illinois funds new communication equipment for Colona police department.** Last week, Illinois Gov. Rod R. Blagojevich announced $13,822 in funding for the Colona Police Department for construction and installation of public safety communications equipment. This is the final installment on a $28,000 grant for the project. "I'm pleased to be able to provide the Colona Police Department with these funds to help meet the community's public safety needs," said Blagojevich. "With the modern technology now available there is no reason for our police officers not to have reliable communications equipment that will ensure their safety and the safety of the residents of Colona." **State Sen. Denny Jacobs, who sponsored the project, said "This new equipment will make it easier for the officers and dispatchers of the Colona Police Department to communicate with each other... "It will also help in the coordination of their efforts with the County Sheriff's Office and the Illinois State Police providing better service and a safer and more secure community."**
Source: http://www.govtech.net/news/news.php?id=89882

16. *April 07, WFTV (Florida)* — **Florida receives $130 million to fight domestic terrorism.** The war on terror got a major boost from the federal government on Wednesday, April 7. The Department of Homeland Security announced more than $100 million coming to Florida to fight domestic terrorism. **Altogether, $130 million is going to help Florida emergency teams better handle terrorism and natural disasters through equipment and training.** Police, fire, and other first responders will receive $92 million. Another $38 million goes to Florida's three big cities. For Orlando and its neighboring counties, that's $9 million, but only if it can coordinate its disaster plan as a team. "In Florida, if terrorists do strike, we have a credible response. But we're not just waiting for it to happen. We're going to prevent it or disrupt it and put the assets on the street to make sure in our communities, we want them to go somewhere else," says Craig Fugate, Florida Division of Emergency Management.
Source: http://www.wftv.com/news/2983480/detail.html

17. *April 07, Federal Computer Week* — **DHS plans info hub.** By summer's end, a federal clearinghouse of information relating to technologies will be rolled out in some form, according to a Department of Homeland Security (DHS) official. The idea for a centralized hub was envisioned in the Homeland Security Act of 2002, which states that a program to promote technological innovation would further the department's mission. "One of the things that we're trying to do is look at how do you collect and disseminate…information in such a way that everybody can find what they need and crosscut those stovepipes especially in these areas where you need to have cross–jurisdictional needs," said Nancy Suski, director of emergency preparedness and response within DHS' Science and Technology Directorate. **Department officials are working with the first responder community to determine their needs and**

with federal agencies to find out what useful information is available.** The clearinghouse would not only be a resource for disseminating information but also for sharing information, providing lessons learned from various government exercises, and offering information on standards and guidelines on best practices, Suski said.
Source: http://www.fcw.com/fcw/articles/2004/0405/web−clearing−04−07 −04.asp

18. *April 07, The Express−Times (PA)* — **Government picks Valley for bioterror program.** Pennsylvania's Lehigh Valley, will serve as a testing ground for a bioterrorism preparedness program intended to become a model for communities nationwide, officials announced Tuesday, April 6. **The three−year Health and Security for the 21st Century Project will focus on improving response and mitigation of bioterrorism and related chemical, biological and nuclear incidents.** "We know that preparation for terror is not a one−time event but an ongoing process. And, to be effective, it has to take place at the local level," said William Gimson, chief operating officer of the Centers for Disease Control and Prevention. The Lehigh Valley was chosen to launch the three−year pilot program because of the region's closeness to high threat regions in Pennsylvania, New York and Washington, DC, and existing infrastructure.
Source: http://pennlive.com/news/expresstimes/pa/index.ssf?/base/new s−10/1081328656317850.xml

19. *April 06, Government Technology* — **Florida data−sharing system helps police nab suspects. A new data−sharing system developed at the University of Central Florida has helped law enforcement officials make more than 70 arrests since October, 2003, while shaving days off the length of some investigations.** By sharing data, the agencies can quickly identify patterns of criminal activity and significantly reduce the time spent investigating crimes. "For years, law enforcement agencies have sought ways to share real−time, operational−level data across jurisdictional boundaries," said Mike Reynolds, associate professor of criminal justice and co−director of the project. Reynolds said the inability to quickly share data across county lines makes it easy for criminals and potential terrorists to go unnoticed.
Source: http://www.govtech.net/news/news.php?id=89879

[Return to top]

Information and Telecommunications Sector

20. *April 08, IDG News Service* — **New Netsky worms change their stripes.** New versions of the Netsky e−mail worm are spreading on the Internet. Netsky.S appeared Monday, April 5, and Netsky.T was detected Tuesday, April 6. They are the 19th and 20th editions of an e−mail virus that first appeared in February. Like its predecessors, **the new Netsky variants target machines running versions of Microsoft's Windows operating system**. The viruses arrive as files enclosed in e−mail messages that have faked (or "spoofed") sender addresses and vague subjects such as "Re: My details," "Request" and "Thank You!" according to anti−virus company Symantec Corp. Earlier versions of the Netsky variant abstained from opening communications ports that could be used as back doors that remote attackers could use to gain access to compromised systems. However, **the latest Netsky variants open a back door on TCP Port 6789 that could be used to receive instructions or malicious code from the worm**

author.
Source: http://www.computerworld.com/securitytopics/security/virus/story/0,10801,91978,00.html

21. *April 06, Federal Computer week* — **Last draft released for security guide.** The National Institute of Standards and Technology (NIST) on April 6 released a final draft of security guidelines for federal agencies that need to certify and accredit their information systems. With May as their target date for publication, **NIST officials cited an urgent need to receive comments on the final draft document by April 21. The proposed guidelines are relevant to security requirements that all federal agencies must meet under the Federal Information Security Management Act of 2002.** NIST officials incorporated several significant changes in the final draft based on earlier comments they received. Among them are newly defined roles for the chief information officer and senior agency information security officer in the certification and accreditation process. Also new are additional guidelines for low−impact information systems, a revised timetable for interim approval to operate information systems, and a summary table of tasks and subtasks for security certification and accreditation. Special Publication 800−37, Guide for the Security Certification and Accreditation of Federal Information Systems, is available online:
Source: http://fcw.com/fcw/articles/2004/0405/web−nist−04−06−04.asp

22. *April 06, Federal Computer Week* — **Industry suggests security improvements.** The Corporate Information Security Working Group, which Rep. Adam Putnam (R−FL) convened five months ago, issued several lists of cybersecurity recommendations that Putnam has promised to review before considering any new security legislation on Tuesday, April 6. **Most of the recommendations from the group's call on the federal government to provide incentives for good corporate security practices, but they reject any substantial role for the federal government in policing the information security practices of corporations.** The group made recommendations on best practices, education, incentives, information sharing and procurement practices. One recommendation was to amend the Clinger−Cohen Act of 1996 to require that federal agencies include computer information security in making IT strategic plans and spending decisions. The recommendations are available online:
http://reform.house.gov/TIPRC/News/DocumentSingle.aspx?Docum entID=3030
Source: http://www.fcw.com/fcw/articles/2004/0405/web−putnam−04−06−0 4.asp

23. *April 06, vnunet.com (UK)* — **F−Secure warns on software flaw.** Security vendor F−Secure is urging users to patch their systems after the discovery of two flaws in a version of its anti−virus software that leaves users vulnerable to hackers and virus writers. **The first flaw could give hackers complete access to a target PC through a hole that affects F−Secure BackWeb 6.31 and earlier versions**. This makes the company's anti−virus, BackWeb and policy management software vulnerable. The second problem is in versions 5.41 and 5.42 of F−Secure's Anti−Virus for MIMEsweeper product. It allows the Sober D worm, which is sent in email−attached Zip files, to bypass the antivirus software and infect PCs. Additional information and a patch available here: http://secunia.com/advisories/11297/
Source: http://www.vnunet.com/News/1154100

Internet Alert Dashboard

[Return to top]

General Sector

24. *April 07, Guardian (United Kingdom)* — **Man jailed over 9/11 is freed.** The only person to have been jailed in connection with the September 11 attacks on New York and Washington was Wednesday, April 7, released from prison, pending a retrial in a German court. **Mounir El Motassadeq, 30, was serving a maximum 15−year prison term in Hamburg after a court in the city convicted him in February 2003 of giving logistical help to the local al Qaeda cell that included three of the September 11 pilots. The guilty verdict was overturned on appeal last month by Germany's federal criminal court and a retrial was ordered.** The federal court ruled that that Motassadeq's conviction on more than 3,000 counts of accessory to murder and membership of a terrorist organization was flawed because the U.S. refused to allow testimony by Ramzi Bin al−Shibh, the alleged September 11 mastermind in their custody. The defendant's lawyers succeeded in securing his release pending the retrial in Hamburg, which is due to begin on June 16.
Source: http://www.guardian.co.uk/alqaida/story/0,12469,1187771,00.h tml

25. *April 07, BBC* — **Iran to press on with reactor. Iran plans to start building a heavy water reactor which could produce weapons−grade plutonium, diplomats say.** Tehran told the head of the UN's International Atomic Energy Agency (IAEA) it would start construction in June, the sources at the IAEA said. Although Iran insists the plant is purely for research, the diplomats say it is a worrying development. One said the plant could produce enough plutonium to make a nuclear weapon each year. Mohamed ElBaradei was told of Iran's plans on Tuesday, during a visit to the Iranian capital, the sources said. The plant would be built in Arak, 200km (120 miles) southwest of Tehran. **ElBaradei has been conducting an assessment of Iran's nuclear ambitions, after the discovery last year that it had not disclosed large−scale efforts to enrich uranium, which can be used in nuclear warheads.**

Source: http://news.bbc.co.uk/2/hi/middle_east/3608817.stm

DHS/IAIP Products &Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP web–site (http://www.nipc.gov), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Warnings – DHS/IAIP Assessements, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Publications – DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other publications

DHS/IAIP Daily Reports Archive – Access past DHS/IAIP Daily Open Source Infrastructure Reports

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883–3644
Subscription and Distribution Information	Send mail to nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883–3644 for more information.

Contact DHS/IAIP

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282–9201.

To report cyber infrastructure incidents or to request information, please contact US–CERT at info@us–cert.gov or visit their Web page at www.uscert.gov.

DHS/IAIP Disclaimer